

برنامه خدا

## اندازه‌گیری اثربخشی مدیریت امنیت اطلاعات

(استاندارد ISO/IEC27004: فناوری اطلاعات، فنون امنیتی،  
سیستم‌های مدیریت امنیت اطلاعات، اندازه‌گیری)

ترجمه و تألیف:  
معزالدین حجت‌الاسلامی

ویراستار فنی:  
علیرضا براثی فرد  
(معاون مرکز توسعه دولت الکترونیک و فناوری اطلاعات وزارت کشور)

## اندازه‌گیری اثربخشی مدیریت امنیت اطلاعات

ترجمه و تأليف: معزالدين حجت الاسلامي

ویراستار، فنی: علی‌ضایی، فرد

ناشر : انتشارات وینا

ناشر همکار: انتشارات آتی نگار

۱۳۹۶، اوایل

شماره ۵۰۰: گارا

پیغامبر

ISBN: 978-964-8816-44-0

حق چاپ برای انتشارات وینا محفوظ است.

نشانی دفتر فروش: خیابان جمالزاده جنوبی، روبروی کوچه رشتچی، پلاک ۱۴۴ واحد ۱

نمبر: ۶۶۵۶۵۳۳۷

تلفن: ٦٦٥٦٥٣٣٦-٨

[www.ati-negar.com](http://www.ati-negar.com) \* [info@ati-negar.com](mailto:info@ati-negar.com)



اندازه‌گیری اثربخشی مدیریت امنیت اطلاعات : استاندارد ISO/IEC27004: فناوری اطلاعات، فنون امنیتی، سیستم‌های مدیریت امنیت اطلاعات، اندازه‌گیری / ترجمه و تالیف [صحیح: ترجمه] معزالدین حجتالاسلامی؛ ویراستار فنی علیرضا براتی‌فرد  
تهران: وینا، آتنی نگر ۱۳۹۶

ISBN: 978-964-8816-44-0

فیا.

یادداشت: عنوان اصلی: - International standard. ISO/IEC 27004, Information technology - Security techniques - Information security management- Measurement

مixin: تکنولوژی اطلاعات = تدابع اینترنت = استانداردها

نیز پر نکاره نام دارد که تواند این را:

موضوع: حفاظت داده‌ها - اسنادداردگان - کامپیوuterها - ایتمی اطلاعات - اسنادداردگان

## موضوع: شبکه‌های کامپیوٹری - تدبیر ایمنی - استانداردها

شناسه افزوده: حجت‌الاسلامی، معزالدین، ۱۳۶۴ - . مترجم

شناسه افزوده، برانی فرد، علیرضا، ۱۳۵۵ - . ویراستار

رده‌بندی کنگره

دہندہ، دیوب

ریاضیات

سماوی سیاستی ملی

# فهرست مطالب

۵	پیشگفتار مترجم
۷	پیشگفتار ویراستار
۹	فصل اول: اندازه‌گیری امنیت
۹	۱-۱ مقدمه
۱۱	۱-۲ نمای کلی مدیریت
۱۱	۱-۲-۱ عدم اختصاص منابع بیش از حد به فرآیند ISMS
۱۲	۱-۲-۲ توصیه‌های استاندارد ۲۷۰۰۴ برای تحقق نیازمندی‌های اندازه‌گیری
۱۲	۱-۲-۳ اندازه سازمان
۱۳	۱-۳ قلمرو استاندارد
۱۳	۱-۴ مراجع اصلی
۱۳	۱-۵ نمای کلی اندازه‌گیری امنیت اطلاعات
۱۳	۱-۵-۱ اهداف اندازه‌گیری امنیت اطلاعات
۱۵	۱-۶ برنامه اندازه‌گیری امنیت اطلاعات برنامه
۱۵	۱-۶-۱ اندازه‌گیری امنیت اطلاعات
۱۶	۱-۶-۲ عوامل موافقیت
۱۶	۱-۷ مدل اندازه‌گیری امنیت اطلاعات (ISMM)
۱۸	۱-۷-۱ معیارهای پایه (B) و روش اندازه‌گیری (M)
۲۰	۱-۷-۲ معیار مشتق و تابع اندازه‌گیری
۲۱	۱-۷-۳ شاخص‌ها و مدل تحلیلی
۲۳	۱-۷-۴ نتایج اندازه‌گیری و ضوابط تصمیم‌گیری
۲۴	۱-۸ مسئولیت‌های مدیریت
۲۴	۱-۸-۱ نمای کلی
۲۵	۱-۸-۲ مدیریت منابع
۲۵	۱-۸-۳ آموزش و آگاهسازی اندازه‌گیری
۲۵	۱-۹ توسعه معیارها و اندازه‌گیری
۲۵	۱-۹-۱ نمای کلی
۲۶	۱-۹-۲ تعریف قلمرو اندازه‌گیری

۲۷.....	۱-۹-۳ شناسایی نیازهای اطلاعاتی
۲۷.....	۱-۹-۴ انتخاب شیء و صفت
۲۹.....	۱-۹-۵ توسعه ساختار اندازه‌گیری
۳۲.....	۱-۹-۶ ساختار اندازه‌گیری

۳۳

## فصل دوم: الگویی برای ساختار اندازه‌گیری امنیت اطلاعات

۳۳.....	۱- الگویی برای ساختار اندازه‌گیری امنیت اطلاعات
---------	---

۳۹

## فصل سوم: مثال‌هایی برای ساختارهای اندازه‌گیری

۳۹.....	۱- آموزش ISMS
۳۹.....	۱-۱ افراد آموزش دیده
۴۲.....	۱-۲ آموزش امنیت
۴۵.....	۱-۳ تطابق آگاهی امنیت اطلاعات
۵۰.....	۲- سیاست‌های کلمه عبور
۵۰.....	۲-۱ کیفیت کلمه عبور - دستی
۵۴.....	۲-۲ کیفیت کلمه عبور - به طور خودکار
۵۸.....	۲-۳ فرایند بازبینی
۶۱.....	۲-۴ بهبود مستمر
۶۱.....	۳-۱ اثربخشی مدیریت رخداد امنیت اطلاعات
۶۳.....	۳-۲ پیاده‌سازی اقدامات اصلاحی
۶۹.....	۳-۳ التزام مدیریت
۷۵.....	۳-۴ محافظت در برابر کدهای بدخواه (برنامه‌های مخرب)
۷۷.....	۳-۵ کنترل‌های ورودی فیزیکی
۸۰.....	۳-۶ بررسی فایل‌های لگ (Log Files)
۸۳.....	۳-۷ مدیریت نگهداری و تعمیر
۸۶.....	۳-۸ امنیت در توافقنامه‌های شخص ثالث

۹۱

## مراجع